Tolérer les fautes Byzantines dans les graphes planaires

Alexandre Maurer, Sébastien Tixeuil

Tolérer les fautes Byzantines dans les graphes planaires

Alexandre Maurer[1,2] et Sébastien Tixeuil[1,2,3]

[1] *Laboratoire d'Informatique de Paris 6 (LIP6)*
[2] *Laboratory of Information, Network and Communication Sciences (LINCS)*
[3] *Institut Universitaire de France (IUF)*
E-mail : alexandre.maurer@lip6.fr, sebastien.tixeuil@lip6.fr

On s'intéresse au problème de la diffusion d'information dans un réseau sujet à des fautes Byzantines : certains nœuds peuvent avoir un comportement malveillant arbitraire. On considère ici les solutions entièrement décentralisées. Une solution récente garantit une diffusion fiable sur une topologie de tore lorsque $D > 4$, D étant la distance minimale entre deux nœuds Byzantins.

Dans ce papier, nous généralisons ce résultat aux graphes planaires 4-connexes. On montre que la diffusion peut être rendue fiable lorsque $D > Z$, Z étant le nombre maximal d'arêtes par polygone. On montre également que cette borne ne peut être améliorée sur cette classe de graphes. Notre solution a la même complexité en temps qu'une diffusion simple. Par ailleurs, c'est la première solution où la mémoire requise augmente linéairement avec la taille des informations, et non plus exponentiellement.

Keywords: Tolérance aux fautes Byzantines, protocole de diffusion, réseaux multi-sauts, réseaux asynchrones

1 Introduction

Motivations Dans un monde où les réseaux deviennent de plus en plus grands, des erreurs locales de fonctionnement sont inévitables. Ces erreurs peuvent avoir des origines diverses : bug informatique, débordement de file, attaque extérieure... Afin d'englober toutes les erreurs possibles, on considère ici le modèle le plus général : le modèle Byzantin [LSP82], où les nœuds fautifs ont un comportement totalement arbitraire. Autrement dit, tolérer les fautes Byzantines implique de garantir qu'il n'existe aucune stratégie, aussi improbable soit-elle, leur permettant de déstabiliser le réseau.

On s'intéresse ici au problème de la diffusion : un nœud (la *source*) souhaite communiquer une information à l'ensemble du réseau. Notre but est de garantir que les nœuds corrects recevront toujours la bonne information, sans jamais être abusés par les nœuds Byzantins.

Solutions existantes Une solution classique est d'utiliser de la cryptographie asymétrique à base de clés publiques et privées [DH76]. Toutefois, outre une certaine puissance de calcul, cela requiert une infrastructure centralisée initialement fiable afin de distribuer les clés. Nous nous intéressons ici aux solutions totalement décentralisées.

Plusieurs solutions [Koo04, BV05, NT09] nécessitent un grand nombre de voisins par nœud, et ne peuvent tolérer plus d'une faute Byzantine sur des topologies faiblement connectées telles que le tore (voir Figure 1). D'autres solutions tolèrent un grand nombre de fautes sur une grille [MT12a, MT13], mais offrent seulement des garanties probabilistes. Une solution récente [MT12b] garantit une diffusion fiable sur un tore lorsque $D > 4$, D étant la distance minimale entre deux nœuds Byzantins.

Notre contribution Dans ce papier, nous généralisons le résultat [MT12b] aux graphes planaires 4-connexes (voir Figure 1). On montre que notre solution de diffusion est fiable lorsque $D > Z$, Z étant le nombre maximal d'arêtes par polygone. On montre également qu'aucun algorithme ne peut améliorer cette borne pour cette classe de graphes. Par ailleurs, on montre que si le délai entre deux activations successives

est borné, la diffusion s'effectue en un temps $O(d)$, d étant le diamètre du réseau. Enfin, on montre que la solution présentée dans ce papier requiert beaucoup moins de mémoire que les précédentes.

Organisation du papier Dans la Section 2, nous présentons les hypothèses et décrivons le protocole exécuté par les nœuds corrects. Dans la Section 3, nous prouvons les propriétés annoncées. Enfin, dans la Section 4, nous montrons une amélioration en terme de mémoire requise. Nous ne donnons ici qu'une esquisse des preuves, mais les versions complètes sont dans le rapport technique disponible à l'adresse : `http://hal.upmc.fr/hal-00773343`

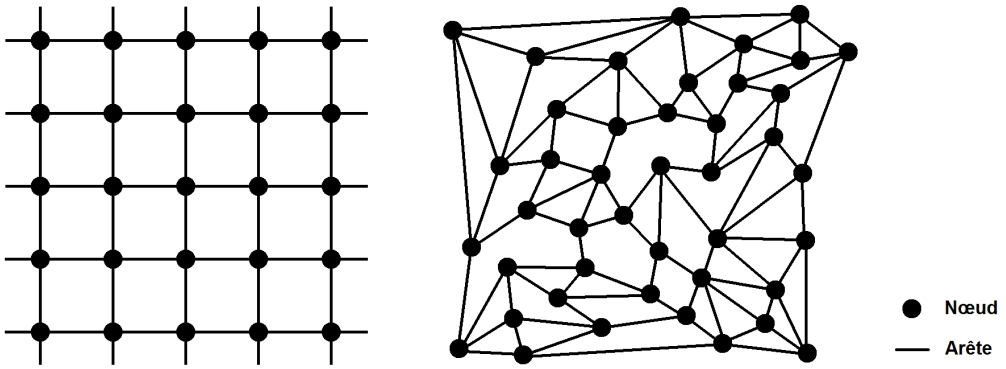

FIGURE 1: Tore (gauche) et graphe planaire 4-connexe (droite)

2 Hypothèses et protocole

Hypothèses On considère que le graphe du réseau est planaire, c'est-à-dire qu'il admet une représentation dans le plan où les arêtes ne se croisent pas. Les arêtes délimitent des polygones (voir Figure 1). Le graphe est 4-connexe : pour déconnecter le graphe, au moins 4 nœuds doivent être enlevés. Soit $Z \geq 3$ le nombre maximal d'arêtes par polygone, et $Y \geq 4$ le degré maximal du réseau.

Certains nœuds sont *Byzantins* et peuvent avoir un comportement arbitraire. Les autres sont *corrects* et suivent le protocole décrit ci-après. On considère un réseau asynchrone : tout message envoyé finira par être reçu, mais cela peut se faire dans n'importe quel ordre. Chaque nœud a un identifiant unique, et les canaux sont authentifiés : lorsqu'un nœud reçoit un message d'un voisin, il connait l'identité de ce voisin.

Principe du protocole Le protocole est sensiblement le même que dans [MT12b]. Le principe est que, pour accepter une information, un nœud doit la recevoir d'un voisin direct, mais aussi d'un autre nœud situé à au plus $Z-2$ sauts. L'idée sous-jacente est que si $D > Z$, les nœuds Byzantins ne pourront jamais coopérer pour faire accepter une fausse information à un nœud correct.

Les messages échangés par le protocole sont de la forme (m,S), m étant l'information prétendument diffusée par la source, et S l'ensemble des nœuds ayant retransmis cette information. Un nœud correct possède, pour chaque voisin q, une variable $Rec(q)$ pour stocker le dernier message envoyé par q.

Description du protocole

1. La source envoie une information m_0 à ses voisins.
2. Les voisins corrects de la source acceptent m_0 et envoient $(m_0,\emptyset)$ à leurs propres voisins.
3. Les autres nœuds corrects ont le comportement suivant :
   - Lorsque (m,S) est reçu d'un voisin $q \notin S$, avec $card(S) \leq Z-3$: stocker (m,S) dans $Rec(q)$ et envoyer $(m,S \cup \{q\})$ aux voisins.
   - Lorsqu'il existe m, p, q et S tels que $q \neq p$, $q \notin S$, $Rec(q) = (m,\emptyset)$ et $Rec(p) = (m,S)$: accepter m, envoyer $(m,\emptyset)$ aux voisins et s'arrêter.

3 Propriétés

Théorème 1 *Si $D > Z$, tous les nœuds corrects reçoivent et acceptent l'information diffusée par la source, et uniquement cette information.*

Esquisse de la preuve On montre d'abord, comme évoqué plus haut, que l'hypothèse $D > Z$ empêche les nœuds Byzantins de collaborer pour faire accepter une fausse information à un nœud correct. Par conséquent, si un nœud accepte une information, ce sera nécessairement la bonne. Reste à montrer que tout nœud correct reçoit effectivement cette information.

On introduit pour cela la notion de chemin polygonal. Un chemin polygonal est une série de polygones connectés par une arête, tels que tous les nœuds de ces polygones soient corrects. On montre tout d'abord qu'avec l'hypothèse $D > Z$, il existe toujours un chemin polygonal connectant un nœud correct donné à la source. On montre ensuite par récursion que la bonne information se diffuse au moins le long de ce chemin polygonal, sinon par un chemin polygonal plus court.

Théorème 2 *Si on a seulement $D \geq Z$, aucun protocole ne peut garantir une diffusion correcte pour la classe des graphes planaires 4-connexes.*

Esquisse de la preuve Considérons le réseau suivant :

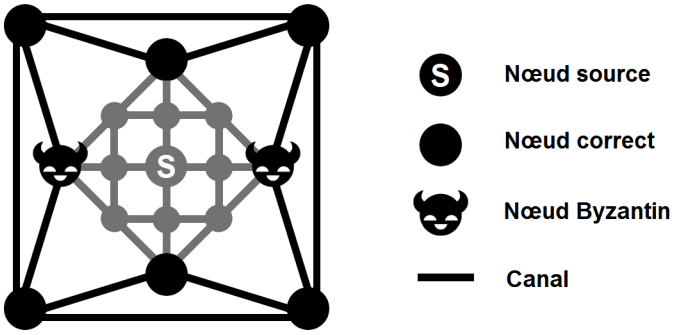

FIGURE 2: Cas critique pour $D \geq Z$

Dans ce réseau, on a $D = Z = 4$, donc a bien $D \geq Z$. Quatre nœuds isolent la partie grise du reste du réseau : deux sont corrects, et deux sont Byzantins. Comme il y a une parfaite symétrie entre ces deux paires de nœuds, les nœuds extérieurs ne pourront jamais déterminer la bonne information avec certitude. Par conséquent, la borne sur D ne peut être améliorée.

Théorème 3 *Si le délai entre deux activations d'un même nœud est borné, alors la diffusion s'effectue en un temps linéaire $O(d)$, d étant le diamètre du réseau.*

Esquisse de la preuve Soit T une borne supérieure du délai entre deux activations. Soit p un nœud situé à $L \geq 1$ sauts de la source. En reprenant la preuve du Théorème 1, on montre qu'il existe un chemin polygonal de Y^3ZL polygones corrects connectant p à la source. On montre ensuite que tous les nœuds d'un polygone correct acceptent la bonne information en un temps Z^2T. On montre finalement par récursion que p accepte l'information en un temps Y^3Z^3TL.

Comme $L \leq d$, et comme Y, Z et T sont bornés, la diffusion s'effectue en un temps linéaire $O(d)$. La complexité en temps est donc la même qu'un protocole de diffusion basique, où toute information reçue est immédiatement retransmise.

4 Mémoire requise

Pour finir, montrons une amélioration de notre protocole en terme de mémoire requise. Dans les solutions existantes [Koo04, BV05, NT09, MT12a, MT12b, MT13], les nœuds peuvent stocker autant d'informations m que nécessaire. Ainsi, comme les nœuds Byzantins peuvent potentiellement diffuser toutes les fausses informations possibles, il faut prevoir $O(2^M)$ bits de mémoire par nœud, M étant le nombre de bits maximal d'une information m.

Dans notre protocole, nous avons fait la modification suivante : au lieu de stocker tous les messages reçus, nous stockons uniquement le dernier message reçu de la part d'un voisin q dans la variable $Rec(q)$. Ainsi, les noeuds requièrent une mémoire de seulement $O(M)$ bits. Quand à la mémoire requise dans les canaux, elle est également de $O(M)$ bits, pour peu que le délai d'activation des nœuds corrects soit compris dans un intervalle $[T_1, T_2]$, $T_1 > 0$. Les canaux liés à des nœuds Byzantins peuvent être débordés sans conséquence, leurs messages étant déjà arbitraires.

La mémoire locale requise augmente donc linéairement avec M, et non plus exponentiellement. Cette modification est propre au cas étudié, nous ne prétendons pas pouvoir l'étendre aux travaux précédents.

5 Conclusion

Dans ce papier, nous avons généralisé la condition sur la distance entre les nœuds Byzantins à une classe de graphes planaires, et montré son optimalité. Notre solution a la même complexité en temps qu'une diffusion simple, et permet d'importantes économies en terme de mémoire locale utilisée.

Un problème ouvert est d'étendre cette condition à des graphes plus généraux. Par ailleurs, bien que l'on ait déjà une complexité en temps linéaire, des optimisations sont envisagées pour réduire le temps de réception.

Références

[BV05] Vartika Bhandari and Nitin H. Vaidya. On reliable broadcast in a radio network. In Marcos Kawazoe Aguilera and James Aspnes, editors, *PODC*, pages 138–147. ACM, 2005.

[DH76] W. Diffe and ME. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976.

[Koo04] Chiu-Yuen Koo. Broadcast in radio networks tolerating byzantine adversarial behavior. In Soma Chaudhuri and Shay Kutten, editors, *PODC*, pages 275–282. ACM, 2004.

[LSP82] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3) :382–401, 1982.

[MT12a] Alexandre Maurer and Sébastien Tixeuil. Limiting byzantine influence in multihop asynchronous networks. *IEEE International Conference on Distributed Computing Systems (ICDCS 2012)*, 2012.

[MT12b] Alexandre Maurer and Sébastien Tixeuil. On byzantine broadcast in loosely connected networks. *International Symposium on Distributed Computing (DISC 2012)*, 2012.

[MT13] Alexandre Maurer and Sébastien Tixeuil. A scalable byzantine grid. *International Conference on Distributed Computing and Networking (ICDCN 2013)*, 2013.

[NT09] Mikhail Nesterenko and Sébastien Tixeuil. Discovering network topology in the presence of byzantine nodes. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12) :1777–1789, December 2009.